

1 What is claimed is:

2 1. A method of managing tool execution via roles on a computer system while  
3 maintaining computer system security, wherein the computer system comprises a  
4 plurality of roles, comprising:

5 delegating one or more tools to a user based on a first role, wherein a  
6 tool provides root access and the first role enables the user to run the  
7 delegated tool(s);

8 identifying one of the plurality of roles to be disabled, wherein the  
9 role identified to be disabled is the first role;

10 accessing the role identified to be disabled so that the status of the  
11 role identified to be disabled may be changed; and,

12 disabling the role identified to be disabled, whereby the status of the  
13 role identified to be disabled is changed, so that the user cannot run the  
14 delegated tool(s).

15  
16 2. The method of claim 1, wherein the first role is represented by a role object  
17 comprising an enablement attribute that has a value that determines whether the first  
18 role is enabled or disabled, wherein disabling the role identified to be disabled  
19 comprises:

20 setting the enablement attribute value so that the first role is disabled.  
21

22 3. The method of claim 2, wherein the user is represented by a user object,  
23 wherein delegating one or more tools to a user based on a role comprises linking the  
24 role object to the user object with an authorization object.  
25

26 4. The method of claim 2, wherein identifying one of the plurality of roles to  
27 be disabled comprises a root user entering, through a command line interface  
28 ("CLI") or graphic user interface ("GUI"), a command that identifies the role object.  
29

30 5. The method of claim 4, wherein the CLI or GUI operate in a process space  
31 and wherein accessing the role identified to be disabled comprises returning the role  
32 object to the CLI or GUI process space.

3                   a)       authorizing the first role for the user, the first role comprising  
4       the delegated tool(s); and

b) authorizing a machine of the computer system for the first role, wherein the computer system comprises a plurality of machines and the user is enabled to utilize the first role only on authorized machines, whereby utilizing the first role comprises running the one or more tools of the first role.

10

11           7.       The method of claim 1, further comprising:

12 identifying one of the plurality of roles to be enabled, wherein the  
13 role identified to be enabled is the first role;

14                accessing the role identified to be enabled; and

15                   enabling the role identified to be enabled, whereby the status of the  
16                   role identified to be enabled is changed, so that the user can run the  
17                   delegated tool(s).

18

19 8. A computer readable medium comprising instructions for managing tool  
20 execution via roles on a computer system while maintaining computer system  
21 security, wherein the computer system comprises a plurality of roles, by:

22 delegating one or more tools to a user based on a first role, wherein a  
23 tool provides root access and the first role enables the user to run the  
24 delegated tool(s);

25 identifying one of the plurality of roles to be disabled, wherein the  
26 role identified to be disabled is the first role;

27                   accessing the role identified to be disabled so that the status of the  
28                   role identified to be disabled may be changed; and,

disabling the role identified to be disabled, whereby the status of the  
role identified to be disabled is changed, so that the user cannot run the  
delegated tool(s).

- 1        9.        The computer readable medium of claim 8, wherein the authorized role is  
2        represented by a role object comprising an enablement attribute that has a value that  
3        determines whether the first role is enabled or disabled, wherein disabling the role  
4        identified to be disabled comprises:  
5                setting the enablement attribute value so that first role is disabled.  
6
- 7        10.       The computer readable medium of claim 9, wherein the user is represented  
8        by a user object, wherein delegating one or more tools to a user based on a role  
9        comprises linking the role object to the user object with an authorization object.  
10
- 11       11.       The computer readable medium of claim 9, wherein identifying one of the  
12       plurality of roles to be disabled comprises a root user entering, through a CLI or  
13       GUI, a command that identifies the role object.  
14
- 15       12.       The computer readable medium of claim 11, wherein the CLI or GUI  
16       operate in a process space and wherein accessing the role identified to be disabled  
17       comprises returning the role object to the CLI or GUI process space.  
18
- 19       13.       The computer readable medium of claim 8, wherein delegating one or more  
20       tools to a user based on a role comprises:  
21               a)        authorizing the first role for the user, the authorized role  
22               comprising the delegated tool(s); and  
23               b)        authorizing a machine of the computer system for the first  
24               role, wherein the computer system comprises a plurality of machines and the  
25               user is enabled to utilize the first role only on authorized machines, whereby  
26               utilizing the first role comprises running the one or more tools of the first  
27               role.  
28

10        15.     A method of managing tool execution via roles on a computer system while  
11        maintaining computer system security, wherein the computer system comprises a  
12        plurality of roles, comprising:

13                   identifying one of the plurality of roles to be enabled, wherein the  
14                   role identified to be enabled is a first role of a user, wherein the first role  
15                   enables the user to run one or more delegated tools, wherein a tool provides  
16                   root access for performing a specific task in the computer system;  
17                   accessing the role identified to be enabled so that the status of the  
18                   role identified to be enabled may be changed; and,  
19                   enabling the role identified to be enabled, whereby the status of the  
20                   role identified to be enabled is changed, so that the user can run the  
21                   delegated tool(s).

23 16. The method of claim 15, further comprising:  
24 identifying one of the plurality of roles to be disabled, wherein the  
25 role identified to be disabled is the first role;  
26 accessing the role identified to be disabled; and  
27 disabling the role identified to be disabled, whereby the status of the  
28 role identified to be disabled is changed, so that the user cannot run the  
29 delegated tool(s).

17. The method of claim 16, wherein the user runs at least one of the delegated tool(s) after the enabling step is performed, wherein identifying one of the plurality of roles to be disabled comprises a root user determining that the user is finished running the delegated tool(s).

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15

18. The method of claim 15, wherein the user is a customer engineer, wherein identifying one of the plurality of roles to be enabled comprises a root user determining that the customer engineer needs to run at least one of the delegated tool(s).

19. The method of claim 15, wherein the first role is represented by a role object comprising an enablement attribute that has a value that determines whether the first role is enabled or disabled, wherein enabling the role identified to be enabled comprises:

setting the enablement attribute value so that the first role is enabled.

20. The method of claim 19, wherein the enablement attribute value is a Boolean value and setting the enablement attribute value comprises setting the enablement attribute value to true.